February 1, 2010

Via ECFS
Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: *GN Docket Nos. 09-47, 09-51, 09-137*
Implementation of Smart Grid Technology and the National Broadband Plan

Dear Ms. Dortch:

Electric power generation, distribution, and consumption patterns are undergoing dramatic and unprecedented changes. Renewable sources of supply, some of which are variable, challenge the existing electric system to cope with multiple and dynamic power sources. The need to more fully utilize kilowatts generated, especially when generated from carbon-based fuel, by ensuring more useable kilowatts pass through the distribution system compels the introduction of intelligence in the distribution and transmission of electricity. The advent of electric-powered vehicles, new conservation initiatives for end users, and the introduction of consumer-as-power-supplier is forcing the grid to generate and manage new kinds of user data that will interact with the grid in ways never before imagined.

These critical and necessary changes in our electric system are inextricably linked to, and depend upon, the Nation's on-going commitment to enable broadband infrastructure across the U.S. In Cisco's view, not only will the new smart grid largely depend upon broadband technologies, but the extension of broadband to all end users is critical to delivering on the power and promise of a broadband-enabled electric system. We will not be able to achieve the full effect of a smart grid without a robust broadband network that connects the supply side with the demand side of the electric industry ubiquitously. The FCC therefore plays a key role in helping to advance the cause of the smart grid.

The IT and electric industries are today engaged in a process of rapid innovation to meet the challenges. Industry estimates that the effort to overhaul the grid will generate 260,000 new jobs, and enhance economic recovery as new hardware and software is created to meet the demands of customers. Cisco equipment and solutions are already playing – and will continue to play – an integral role in the transition of the United States' electric power system to a smart grid. Cisco is working with electric power utilities that are integrating communications capabilities into their networks, and with communications companies that are partnering with electric utilities to provide the communications capabilities necessary to modernize the power generation and distribution systems.

Based on Cisco's extensive experience with developing complex networking communications platforms, in our view the deployment of smart grid technologies is still in its early stages, and will certainly continue to evolve over time. This filing represents Cisco's current perspective on the following significant smart grid issues that relate to questions raised, and dialogue we have participated in, with FCC leaders and other policy makers: (1) basic structure of smart grid communications technologies, including the role of spectrum-based technologies and home area networks ("HAN"); (2) security and critical infrastructure concerns; and (3) economic models around cost recovery.

I. The Smart Grid is a Network of Networks

In considering smart grid issues, it is important to bear in mind that "the" smart grid will actually be a network of networks, much like the Internet in structure. For the thousands of utilities across the U.S., an architecture similar to the Internet, which is based on the Internet Protocol (IP) and is open and interoperable, is critical to achieving a smart grid. In Cisco's view, the smart grid, like the Internet before it, needs a control plane, and we believe that control plane should be digitized and use IP. In our view, this is the only solution that can support interoperability, resiliency, and security, issues that are critical to the highly-regulated electric utilities. We believe this should be the basis upon which the Commission bases its regulatory approach. One Size Does Not Fit All.

It is judicious for the Commission to gather and review information related to the current state of the grid and innovation that is just now rolling out to enable the smart grid, as we also anticipate an array of communications policy matters that could either accelerate or delay the vision. At the same time, it is important to remember that the smart grid is a relatively new initiative, and like the Internet, the fewer the regulatory barriers in its path, the better. In fact, efforts to integrate existing information exchange and control systems in the grid and to broaden their deployment are just beginning. While more uniform and interoperable systems are an appropriate goal, the Commission must account for the multiplicity of existing architectures.[1]

To date, electric utilities have deployed a variety of systems to use broadband and communications technology to improve the performance of electricity transmission and distribution facilities, more often using proprietary protocols with solutions that are customized. One goal of smart grid technology must be to connect the islands of data found in the current electrical grid, as well as new data that will be generated from smart grid technologies. As the Commission is well aware, the National Institute of Standards and Technologies ("NIST") received a substantial grant through the American Recovery and Reinvestment Act ("Recovery

[1] *See* NBP PN #2, Question 1.

Act") to develop standards for smart grid interoperability (an effort originally authorized by the Energy Independence and Security Act of 2007).[2]

In the context of the NIST proceeding, Cisco has supported an integration, and ultimately a migration, of existing technologies and solutions to an end-to-end, IP-based smart grid architecture.[3] IP-based architectures are scalable, extensible and reliable, and can support the necessary security standards. They also can be backwards-compatible with legacy systems and networks, which is important for a number of reasons. First, it protects utilities' existing investments in information exchange technology, which both benefits ratepayers and avoids penalizing utilities for being smart grid "early adopters." Second, backwards-compatibility allows smart grid product cycles to run their natural course, and prevents a potentially disastrous "hard stop" in equipment purchases that could result if utilities perceive an impending, specific technology mandate. Thus, while an IP-based system that leverages Internet architecture and new investment should be the ultimate goal, legacy systems must also be supported and migrated into an IP-based smart grid architecture over time.

Cisco is therefore pleased that NIST has identified, in its final *Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*[4], the Internet Protocol Suite including, but not limited to: IETF RFC 2460 (IPv6)[5], IETF RFC 791 (IPv4)[6] and the Core Protocol in the Internet Suite, draft-baker-ietf-core-04[7] as interoperability standards suitable for use in the smart grid.

Smart grid technology must serve different types of customers and widely different types of network topologies. The Commission's approach should recognize the diversity of solutions and embrace policies that are pro-consumer and pro-innovation, while recognizing the need for utilities to meet shareholder expectations.

A. Spectrum-Based Technologies in the Smart Grid

The Commission has sought to understand how wireless spectrum is or could be used for smart grid applications.[8] As discussed below, wireless networks provide important functions, such mobility and redundancy. A variety of different types of spectrum – licensed and

[2] 42 U.S.C. § 17381 *et seq*.

[3] *See Internet Protocol Architecture for the Smart Grid*, Cisco Submission to the National Institute of Standards and Technology ("NIST"), (July 9, 2009), *available at* http://www.cisco.com/web/strategy/docs/energy/CISCO_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf (last visited Oct. 22, 2009).

[4] *See* http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf (last visited Jan. 26, 2010).

[5] *See* http://www.ietf.org/rfc/rfc2460.txt (last visited Jan. 26, 2010).

[6] *See* http://www.ietf.org/rfc/rfc791.txt (last visited Jan. 26, 2010).

[7] *See* http://tools.ietf.org/html/draft-baker-ietf-core-04 (last visited Jan. 26, 2010).

[8] NBP PN #2, Question 3.

unlicensed, utility-owned and carrier-owned – is currently being used for smart grid deployments. Each of these existing technologies and networks has merit, and no single solution appears to solve the diverse needs of the smart grid.

Utility of Wireless Networks for Smart Grid. An analysis of the merits and demerits of wireless networks in the smart grid context are generally very similar to such an analysis in any other context. Briefly stated, wireless networks provide the potential for mobility, and can often be deployed to serve a given geographic area less expensively than fixed-line networks. At the same time, the laws governing the propagation of electromagnetic signals inevitably make wireless networks less reliable than their fixed counterparts under certain circumstances. These factors must be balanced appropriately.

As the Commission is well aware, electric utilities are subject to extensive reliability regulation at multiple levels, including the Federal Energy Regulatory Commission ("FERC")[9] and the various state public utilities commissions.[10] Thus, communications networks for smart grid applications must be highly reliable. In Cisco's experience, this level of reliability is possible from wireless networks, including both utility-owned and commercial networks. In addition, even where fixed broadband or telecommunications infrastructure is deployed, wireless networks can provide redundancy, further improving reliability and enhancing customer care capabilities such as improvements on outage times.

Licensed Spectrum. Some promising smart grid technologies are evolving that use licensed spectrum. A brief survey of these, based on Cisco's experience and learnings, is below.

Electric Utility Systems

Electric utility companies in the U.S. operate numerous legacy, proprietary systems (dating from mid-20th century) that utilize both licensed and unlicensed spectrum to support their operations. Some of these networks use unlicensed radio solutions, such as wireless mesh networks, to obtain data from meters and send the data over licensed point-to-point microwave systems.[11] Electric utilities hold numerous authorizations to operate communications facilities in the Private Land Mobile Radio ("PLMR") Services. In fact, the Power Radio Service ("PRS") was created for the exclusive use of public utilities, including electric utilities, with substantial frequencies below 500 MHz dedicated for PRS use.[12] Electric utilities also utilize multiple

[9] *See* http://www.ferc.gov/industries/electric/indus-act/reliability.asp (last visited Oct. 22, 2009).

[10] *See*, for example, http://www.cpuc.ca.gov/PUC/energy/ElectricSR/Reliability/pro_desc.htm (last visited Oct. 22, 2009).

[11] *See* Comments of Utilities Telecom Council, GN Docket 09-47, at 7-8 (Oct. 2, 2009) ("UTC Comments").

[12] *See* former 47 C.F.R. § 90.63 (1986). The Commission eventually consolidated the twenty PLMR services into two general pools consolidation of the twenty PLMR Services into two pools -- one for Public Safety and one for Industrial/Business. The PRS was consolidated into the Industrial/Business pool. *See Replacement of Part 90 by Part 88 to Revise the Private Land Mobile Radio Services and*

address systems ("MAS"), which are point-to-multipoint communications systems licensed under Part 101 of the Commission's Rules, to monitor their power lines for faults or blockages through supervisory control and data acquisition ("SCADA") systems.[13] These types of operations, however, generally operate at relatively low speeds. For example, SCADA systems generally transmit only 256 bytes of data and can operate with a latency approaching 2 seconds.[14]

<u>Terrestrial commercial mobile radio services</u> (Cellular, PCS, licensed WiMAX™)

Licensed, terrestrial commercial mobile radio services ("terrestrial CMRS") have become integrated into a number of smart grid solutions. Solutions that utilize terrestrial CMRS networks are becoming more popular because of the high security associated with the networks[15] and new pricing plans for smart grid applications which substantially reduce the traditional cost associated with using these systems.[16] For example, AT&T and T-Mobile USA, Inc. ("T-Mobile") have entered into arrangements with various smart meter manufacturers pursuant to which smart meters are designed to transmit data from customer locations over terrestrial CMRS networks.[17] Terrestrial CMRS networks also are being used to transport real-time performance data from outage monitors and voltage sensors.[18]

Further, terrestrial CMRS networks are being utilized to provide backhaul and SCADA communications that were traditionally carried over proprietary electric utility networks. For

Modify the Policies Governing Them, PR Docket 92-235, *Second Report and Order,* 12 FCC Rcd 14307, 14308-09 (1997).

[13] *See Amendment of Rules to Eliminate Grandfathering Provisions Applicable to Licensees on MAS Frequencies,* PR Docket No. 90-260, *Report and Order*, 6 FCC Rcd 3721, ¶ 2 (1991).

[14] *See* UTC Comments at 6.

[15] *See* Comments of National Rural Electric Cooperative Ass'n, GN Docket No. 09-47 at 7-8 (Oct. 2, 2009) (stating that "[t]he high security that PCS offers is especially attractive to Electric Co-ops for medium-bandwidth applications").

[16] *See, e.g.,* Fierce Wireless, *AT&T To Offer Wireless Smart Grid Technology To Utility Companies* (March 2009), *available at* http://www.fiercewireless.com/press-releases/t-offer-wireless-smart-grid-technology-utility-companies-0 (last visited Oct. 20, 2009).

[17] *See* http://www.fastcompany.com/blog/ariel-schwartz/sustainability/t-mobile-joins-smart-grid-wireless-network-brigade (last visited Oct. 20, 2009); http://earth2tech.com/2009/04/16/phone-companies-heart-smart-grid-smartsynch-att-sign-up-texas-utility (last visited Oct. 20, 2009). Mobile virtual network operators ("MVNOs") have also been established to satisfy demand for smart grid applications operating over terrestrial CMRS networks. *See* http://earth2tech.com/2009/04/16/phone-companies-heart-smart-grid-smartsynch-att-sign-up-texas-utility.

[18] *See* http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=26874 ("AT&T/Cooper Press Release") (last visited Oct. 20, 2009); http://www.greentechmedia.com/articles/read/att-links-cooper-power-systems-smart-grid-devices (last visited Oct. 20, 2009). Under the CPS agreement, AT&T will co-sell the outage monitors and voltage sensors. AT&T/Cooper Press Release at 1.

example, Verizon Wireless has entered into agreements whereby it will carry the backhaul traffic from mesh networks utilized in various smart grid deployments.[19] Sprint and AT&T also have announced solutions that carry SCADA communications.[20]

It is worth noting that participation in providing smart grid solutions is not limited to the traditional terrestrial CMRS carriers. Arcadian Networks touts a solution that utilizes recently-licensed 700 MHz spectrum to provide "a single ubiquitous 'cloud'" that can be used to satisfy numerous smart grid applications.[21] Moreover, there is substantial electric utility interest in exploring the use of WiMAX networks to support smart grid applications.[22]

Unlicensed/Shared Spectrum. Unlicensed spectrum also supports some important smart grid applications. These generally fall into four broad categories:

- 3.65 GHz WiMAX: In the U.S. this spectrum is available on a "lightly licensed" basis (license required but operations are not exclusive). Significantly, spectrum from 3.5-3.6 GHz is a WiMAX Forum™ "profile" and has a global footprint, so that equipment deployed in this band would likely be able to take advantage of global economies of scale.

- 900 MHz: Spectrum in this band is used by many smart metering companies; there are significant numbers of utilities that use this technology today.

- 2.4 GHz: This is the home of Wi-Fi® using the IEEE 802.11 or 802.15.4 standards, which can be used for a wide variety of applications, including those related to smart grid; smart metering applications are particularly prevalent here.

[19] *See* http://tdworld.com/info_systems/vendor_updates/verizon-ambient-smart-grid-0309 (last visited Oct. 20, 2009); http://www.greentechmedia.com/green-light/post/verizon-itron-hook-up-smart-grid-communications-1315 (last visited Oct. 20, 2009).

[20] *See* http://www.wireless.att.com/businesscenter/solutions/industry-solutions/vertical-industry/scada.jsp (last visited Oct. 20, 2009); http://www.energycentral.com/intelligentutility/scada/news/vpr/7557/Sprint-Supports-Utility-Smart-Grid-Initiatives-across-America (last visited Oct. 20, 2009).

[21] *See* http://www.arcadiannetworks.com/article.aspx?MID=3000&CID=5018 (last visited Oct. 20, 2009).

[22] *See* http://earth2tech.com/2009/09/11/utility-interest-in-wimax-for-smart-grid-growing (last visited Oct. 20, 2009). In addition to terrestrial CMRS, the satellite industry is now beginning to express interest in smart grid applications, including both meter reading and SCADA. *See* http://viasatellite.com/broadband/headlines/Hughes-Launches-Broadband-Management-Service-to-Aid-in-Smart-Grid-Efforts_30481.html (last visited Oct. 20, 2009); http://www.bloomberg.com/apps/news?pid=20601087&sid=atXwQrupCu4s (last visited Oct. 20, 2009).

- 217-220 MHz: This spectrum is primarily licensed to the ship-to-shore service, but Adapt4, LLC is a "secondary" licensee, deploying proprietary and cognitive technology that is marketed to utilities, among others.

As the market leader in unlicensed 802.11 devices for use in the 2.4 GHz band, Cisco also wishes to address questions that have been raised regarding interference potential, and thus the suitability of this band and protocol, for utility applications. In Cisco's view, interference concerns are misplaced. The 802.11 standard is a "contention-based" protocol, which means that, if packets are missed as a result of simultaneous use of a channel by different devices, they are simply requested by the receiving device and re-sent. Thus, an increase in simultaneous users does not fundamentally affect the reliability of the data transfer; it potentially decreases the speed of the data flow, although in most cases not to a level even detectable by the user

The Commission has already recognized how robust 802.11 technology is, in adopting rules allowing it to be used for public safety broadband at 4.9 GHz. For example, in a public safety simulation involving multiple emergency vehicles in close proximity to one another, including a remote-controlled bomb-defusing robot with streaming video, all using Wi-Fi connections and sharing 50 MHz of spectrum, no performance degradation was observed. In fact, as we understand it, the concerns around interference in the smart grid appear to be related more to the interaction of 802.11 technology with other unlicensed technologies, in particular, certain types of cordless phone technology. In our experience, evolution in cordless phone technology has largely addressed this concern.

Need for Additional Spectrum. The Commission has inquired whether additional spectrum is required for smart grid applications and, if so, why current allocations are inadequate.[23] In Cisco's experience, the data transfer and communications functions that smart grid demands are not significantly different from other applications. Legacy networks, including standards-based technologies, support some of these applications today, and as the transition to IP-based networking on the smart grid proceeds, it appears that advanced wireless technology platforms available today or in the near future are likely to have sufficient bandwidth and quality-of-service to support evolving smart grid needs for the foreseeable future. Thus, additional spectrum is not needed to deploy technology that is unique or specific to smart grid applications, *per se*. In our view, the decision about whether to allocate additional spectrum rests entirely on other decisional factors – i.e., whether the Commission believes the use case has been justified for smart grid-specific spectrum in light of other demands on radio spectrum.

Global Spectrum Coordination.[24] As noted above, certain spectrum allocations that are used for smart grid applications, both licensed and unlicensed, are consistent with usage in other countries for similar purposes. In Cisco's experience, while global harmonization is not necessary to ensure a viable U.S. market, it has certain advantages. All other things being equal, a potentially global universe of vendors leads to a larger ecosystem, more competition, an increase in the diversity of offerings, greater innovation, and lower costs for both utilities and

[23] NBP PN #2, Question 3.f.

[24] NBP PN #2, Question 3.f.v.

rate payers. At the same time, spectrum that is not globally-harmonized is currently being used successfully for smart grid applications.

B. Home Area Networks

A critical part of leveraging the power of the new smart grid will be its extensibility into the home or end user environment. This is much more than empowering consumers to take action to become more efficient users of energy. It is also about the exchange of information that will need to occur between end users and utilities. For example, the introduction of smart electrically-powered vehicles will reduce carbon footprints, but consumers will need a way to charge their vehicles at locations away from their licensed address. In some way, the device (in this case, the electric car) will need to generate information about itself that will allow the consumption of electricity to be charged to the owner or operator of the vehicle. Of course, incenting efficiency in home energy consumption will also require the exchange of data. As in other smart grid domains, Cisco anticipates that the HAN will feature multiple types of technologies and diverse architectural approaches that will likely evolve over time.

In certain smart grid pilot programs, Home Area Networks may feature the following components, such as:

- A smart meter
- An in-home display
- A smart thermostat
- Smart plugs and switches (i.e., devices that can be attached to a home appliance in order to measure power consumption and also control it)
- Smart appliances (e.g., hot water heater)
- A home energy controller, which provides the networking of connected devices – such as smart appliances, smart thermostat, the smart meter, etc. – as well as their applications, such as energy monitoring, and device command and control.

Most networking technologies in the home consist of traditional home networking protocols (WiFi and Ethernet), protocols currently being used in HAN trials (e.g., ZigBee®, HomePlug®), home automation protocols (e.g., Z-Wave®, X.10) and a number of proprietary protocols used by meter vendors (e.g., Itron Encoder-Receiver-Transmitter™). To facilitate innovation in the HAN, Cisco believes that the Internet Protocol (IP) is the most secure, scalable, and flexible communications platform solution and recommends that future network design for the HAN supports IP (e.g., ZigBee® Smart Energy 2.0, etc.).

The Home Area Network is receiving a great deal of attention from technology companies and utilities to determine which solutions will emerge as the most impactful, scalable, secure, cost effective, and interoperable. A significant amount of work must occur in the HAN domain, which sits at the intersection of the utility grid, the in-home electric network, and the devices that operate in the home. The multiplicity of players, and the multiplicity of potential solutions, makes this subject area one of the most challenging in terms of deploying a smart grid.

In Cisco's view, HAN development is still in its early days. To begin to familiarize ourselves with the HAN, Cisco has partnered with a German utility on a smart grid pilot project to enable 70 residential and business customers to communicate directly with the local power grid, to measure the amount of electricity appliances are using, and to control and manage consumption. Participating homes are being equipped with "smart plugs" to allow consumers to schedule their energy consumption by deferring their use to off peak hours. Home energy management "dashboards" will allow customers to look at their consumption patterns and set rules for appliance use. IP networks will securely transmit data between the utility and the end users.

Projects such as these are also important because the technology allows consumers to be a supply source for electricity, as well as a consumer of it. Rooftop solar panels and wind systems will increasingly be used by residential consumers to generate power, and excess capacity can flow into the grid. But to take full advantage of this dynamic and variable source of supply, the grid will need to be much more sophisticated.

II. Security

Security is an important consideration related to the deployment of smart grid technology and the National Broadband Plan.[25] Although smart grid communications can assist in transforming the energy industry, playing a critical role in maintaining high levels of reliability, performance, and manageability, integration of communications into the grid also introduces the need for an integrated security infrastructure. Many of the technologies being deployed to support smart grid projects—such as smart meters, sensors, and advanced communications networks—have the potential to increase the vulnerability of the grid to attack. The development of a diverse set of networks to support the integration of micro-grids, open-access energy competition, and the use of network-controlled devices is driving the need for a converged security infrastructure for all participants in the smart grid, including utilities, commercial businesses, consumers, and energy service providers. Securing the assets of electric power delivery systems, from the control center to the substation, to the feeders and even to customer meters, requires an end-to-end security infrastructure that protects the myriad of communication assets (e.g., control center-based SCADA, RTUS, PLCs, power meters, digital relays, and bay controls) used to operate, monitor, and control power flow and measurement.

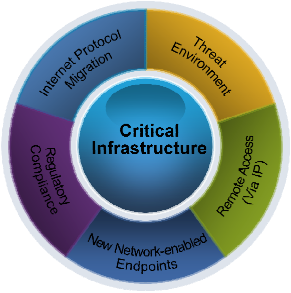
It is a fallacy, however, that a smart grid is less secure than today's grid – that by migrating the energy network to IP, critical infrastructure could be exposed to the dangers of the Internet. The reality is that using IP as a communications protocol is not the same as putting the energy grid on the Internet. In fact, in Cisco's view, the knowledge base and history of how to secure IP networks already exists, and the energy industry can effectively use this knowledge.

[25] *See* NBP PN #2, Questions 3.f.iv., 4.c.

The benefits of this approach far outweigh the risks. To the extent these controls are properly implemented, energy providers can confidently build truly secure networks that ultimately deliver on the promise of a smart grid.

As the process of migrating to a common IP infrastructure accelerates across the industry, it is important to understand the need for security and also define a set of effective security controls. The North American Electric Reliability Corporation ("NERC") has published a set of compliance standards for critical infrastructure protection ("CIP").[26] These standards are still maturing and subsequent revisions are in process. Other governing bodies have initiated or are participating in standards activities. These and other activities illustrate the importance of developing standards and regulations and are vital to building a successful security strategy.

An effective security strategy for the smart grid needs to be end to end and to converge both physical and cyber security requirements. This means that security capabilities need to be layered such that defense mechanisms have multiple points to detect and mitigate breaches. Cisco thinks about security on the grid in the following way:



Cisco's View of Security & the Grid

- Provide security architectural framework (SAFE)
- Cyber security solutions (firewalls, IPS, VPN, identity, access control)
- IP-converged physical security portfolio (Video surveillance, alarms, centralized control)
- Deliver hardened network devices and systems
- Real-time monitoring, management, and correlation via Cisco Security Intelligence Operations (SIO)

These capabilities also need to be integral to all segments of the grid infrastructure and address the full set of logical functional requirements, including:

- *Physical security*: Attacks from a smart grid could come from within as well as from external sources. Electronic access control, video surveillance, and emergency response systems will be future assets to protect our nation's critical infrastructure.
- *Identity and access control policies*: Valid users of smart grid equipment may include utility employees, contractors, and customers. Access to these user groups, whether locally or remotely, should be granular and controlled, and should provide access only to "need to know" information. Strong authentication controls can be put in place to implement these requirements.

[26] *See* http://www.nerc.com/page.php?cid=2|20.

- *Hardened network devices and systems*: Networking devices such as routers and switches can be points of vulnerability unless they are properly configured. Utilities should adopt "effective best practices" to ensure the proper security of every device on the network.

- *Threat defense*: A comprehensive threat defense strategy is required to broadly cover the diverse and constantly evolving vulnerabilities that operators of a smart grid network will face. Despite discrete functional zones and clear segmentation, it is often difficult to anticipate what form a new threat might take. Therefore, it is important to apply security principles broadly across the entire network infrastructure to build an effective, layered defense.

- *Data protection for transmission and storage*: There needs to be enforcement of security policies that permit information sharing between grid segments and secure access for administrative personnel. The primary security technologies that enable this are firewall, VPN, and host-based security for server protection.

- *Real-time monitoring, management, and correlation*: For ongoing maintenance and tighter control, it is important to have the ability to monitor events at a granular level. Over the lifespan of any complex system, events happen that impact the ability of the system to function. Just as in the case of the Internet, where, for example, there might be a cut to an underwater cable or a denial of service attack, it is critical that the smart grid be enabled with tools that will allow grid managers to cope with unforeseen events. Some of these events might be the result of a security incident, and some might simply be "noise," but it is important for the system to detect those events, generate alerts, set priorities and apply intelligence so that more informative and intelligent decisions can be made. This level of visibility can show which network elements are being targeted, which network elements might be vulnerable, and what type of corrective action needs to take place. This is a requirement for any successful security strategy.

While future challenges to grid security are real, they are surmountable and can be anticipated based on the learnings and history of many other network deployments from other industries. Cisco's experience with addressing similar concerns in migrating telephone and secure data networks to IP-based systems is directly relevant here. In the National Broadband Plan, Cisco recommends that the Commission recognizes, encourages, and defers to ongoing industry efforts to develop appropriate security standards for smart grid technologies.

III. Utility Incentives to Deploy Smart Grid Technologies

While cost recovery and economic incentives are not issues that the Commission raised in its Public Notice seeking targeted comment on smart grid issues, we believe these issues should be considered in the National Broadband Plan. Many smart grid investments – like any investments that increase energy efficiency – present significant incentive issues for electric utilities, because they reduce usage of the utility's primary product or create new competitive forces in the energy market. Given the critical national purpose goals that these investments serve, however, it would be useful for the National Broadband Plan to focus attention on the importance of addressing the challenge around the incentive problem and the opportunities we have to overcome them. While the $4.5 billion in Recovery Act funding directed to smart grid grant programs will serve as an important "down payment" toward the development of a smart grid – and ideally, will help answer the multitude of pending technology, standards, security, and business model questions – the real work of deploying a smart grid will come from 'smart regulation' and even 'smarter deregulation' by state utility commissions.

In 2007, a joint working group convened by the Department of Energy ("DOE") and the Environmental Protection Agency ("EPA") studied this issue and produced a report, "Aligning Utility Incentives with Investment in Energy Efficiency."[27] This report collected the various cost recovery practices of the state regulatory commissions associated with energy efficiency incentives, and further identified a subset of practices that appeared to produce the greatest consumer welfare gains. Inherent in the document is the recognition that there is no single cost recovery practice that should be used in all cases and for all utilities. This report is now more than two years old, and thus pre-dates most of the intensive recent work in the smart grid area. Cisco therefore suggests that the FCC include in the National Broadband Plan a recommendation that the Senate and House Committees of jurisdiction direct DOE and EPA to review this issue based on current circumstances and present an updated report. Further, given rapid changes in technology and other factors, the analysis should be refreshed at regular, timely intervals thereafter.

* * *

We hope that this information is useful to the Commission's efforts in producing the National Broadband Plan. Please do not hesitate to contact Cisco with any questions.

Respectfully Submitted,

Cisco Systems, Inc.

By: Jennifer Sanford
Mary Brown
Cisco Global Policy and Government Affairs
1300 Pennsylvania Avenue, NW, Suite 250
Washington, DC 20004
202-354-2928
jennsanf@cisco.com
marybrow@cisco.com

CC: Nick Sinai

[27] Dept. of Energy and Environmental Protection Agency, "Aligning Utility Incentives with Investment in Energy Efficiency" (Nov. 2007), available at http://www.epa.gov/RDEE/documents/incentives.pdf.